ATTACHMENT A1 – Facebook, Inc.

This warrant applies to information associated with the Facebook account "HISROYALFINEST" at https://www.facebook.com/HISROYALFINEST, that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a business headquartered at 1601 Willow Road, Menlo Park, CA 94025

ATTACHMENT B1 - Facebook, Inc.

I. Files and Accounts to be produced by Facebook, Inc. for the period August 23, 2005 to the present.

To the extent that the information described in Attachment A1 is within the possession, custody, or control of Facebook including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Facebook or have been preserved pursuant to a preservation request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A1:

a. Any and all associated subscriber information and user contact info, including, but not limited to, all "About Me" data, user identification number, current name and any prior names associated with the Target Account(s), alternate names, birth date, contact email addresses, including removed email addresses, physical addresses, associated or registered telephone numbers, associated screen names, associated websites, apps, registration date, and work data;

b. A user "neo-print," including account status history, profile contact information, date and time of account creation, historical login information, mini-feed, status update history, shares, notes, wall and timeline postings to the Target Account(s), wall and timeline postings made by the Target Account(s) to other accounts, friend listing, including deleted or removed friends and friends identified as "Family," the names of all users listed as "Followers" or as "Following," networks, groups listing, future and past events, and video listing;

c. A user "photo-print," including all undeleted or saved photos, photos in which the user has been "tagged" with the user name, and all associated metadata or EXIF data with any such photos;

d. Any and all associated Groups information, including a list of all other users currently registered in any such groups and the current status of the group profile;

e. Any and all public or private messages, including any attached documents, images, or photos, including from the Facebook Messenger app, the Facebook mobile app, and the Facebook website accessed via mobile device (including phone or tablet) or computer;

f. All notes written and published to the Target Account(s);

g. All Internet Protocol ("IP") logs for the Target Account(s) from @@ to the present, including script data, script get data, user ID, view time, IP source information, login and logout data, and active sessions data;

h. All chat history, including, but not limited to, the content of all chats and date and time information for all chats, including from the Facebook Messenger app, the Facebook mobile app, and the Facebook website accessed via mobile device (including phone or tablet) or computer;

i. All check-in data;

j. All Connections data, including, but not limited to, all users who have liked the Page or Place of the Target Account(s);

k. All stored credit card numbers;

l. All Events data;

m. All Friend Requests data, including pending sent and received friend requests;

n. All associated data that is "Hidden from News Feed," including any friends, apps, or pages hidden from the News Feed;

o. The last location associated with an update;

p. All "Likes on Other's Posts," "Likes on Your Posts from others," and "Likes on Other Sites" data;

q. A list of all linked accounts;

r. A list of all "Pages You Admin" for the accounts listed below;

s. All Physical Tokens data;

t. All Pokes data;

u. All Recent Activities data;

v. All Searches data;

w. All Shares data;

x. All videos posted to the Target Account(s);

y. The subscriber's registration information provided at time of account creation, including IP address(es);

z. The subscriber's service and account information, including any billing address(es) provided, billing records, telephone numbers, IP address (at each transaction), and complete transactional information;

aa. The subscriber's email address(es) and/or any email address(es) relating to the subscriber;

bb. The subscriber's records of session times and durations and any information relating to the session including, but not limited to, any temporarily assigned network address, Internet Protocol (IP) address, MAC address;

cc. The subscriber's length of service (including start date) and types of services utilized and any information associated with that service such Internet Protocol (IP) address, MAC address, Caller ID, and Automatic Number Identification (ANI);

dd. The subscriber's means and source of payment for any financial transactions (including any credit card or bank number);

ee. IP addresses and location data for all posts, wall posts, comments, friend requests, all messages and electronic communications, photo uploads, likes, Messenger messages and file transfers, and machine cookie information; and

ff. Interstitial Facebook, Facebook Messenger, and Instagram accounts linked to the Target Account(s) by usernames, e-mail addresses, SMS numbers, credit card numbers, bank account numbers.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the account described in Attachment A1 which is evidence, fruits, and instrumentalities of violations of theft of government property and wire fraud including:

a. All records, information, documents or tangible materials regarding:

1. Communication between the target account(s) and other coconspirators, known or unknown;
2. Email accounts, user names, or profiles associated with other coconspirators, known or unknown;
3. Schedules, plans, meetings, communications, or activities while traveling outside or inside the United States;
4. Financial records, benefits, documents, or statements related to the use of government benefits;
5. Photo, videos, or other media featuring RICH, their children, spouses, or parents;
6. Steps taken by RICH, or any other coconspirators to conceal their scheme from law enforcement or government officials; and,
7. Use of any fraudulent documentation to receive money or benefits.

b. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

c. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

d. Evidence of the times the account was used;

e. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

f. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;

g. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account; and,

h. All “address books” or other lists of contacts.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose

those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.